2600 APRIL, 1986

VOLUME THREE, NUMBER FOUR $2

RSTS For Beginners

by The Marauder

RSTS/E is an acronym for Resource System Time Sharing Environment. It is an operating system, most commonly found running on Digital Equipment corporation's (DEC) PDP series of computers (i.e. PDP-11/70 being quite common.). This article describes the basics of identifying, obtaining entry, and some basic things to do once you are in a system running RSTS/E.

System Identification

Upon connection to a RSTS/E system, it will usually identify itself with a system header similar to:

KRAMER CORP. RSTS/E V7.2 JOB 5 KB32: (DIAL-UP) 18-FEB-84 3:46 PM
User:

So as you can see, an RSTS/E system is quite easily recognized due to the fact that it actually tells you in the system header. It is possible for the system manager to modify the login to not display this information, but very few systems do not print out a standard system header. If it has been changed, it will most likely still display the 'user:' prompt. Note: it's also not entirely uncommon for RSTS systems that prompt for a user number to use the "#" character. In either case once you have reached the user: (or "#") prompt, RSTS/E is now awaiting you to enter a valid user (account) number. Once you enter a valid PPN, RSTS will prompt you with: "Password:". If you enter both a valid account, and its matching password, you're in.

Login/Account/Password Formats

An account on an RSTS system is always two numbers between 0 and 255 (inclusively) separated by a comma. This is normally referred to as the Project-Programmer Number or PPN. The first number is the Project Number, and the second is the Programmer Number. Some examples of valid PPN's are: 200,200; 50,10; 30,30; or 1,7.

Passwords on RSTS/E system are always 1 to 6 characters long and can include: the upper case letters 'A-Z', the numbers '0-9', or a combination of both. No lower case letters, and no special characters are allowed (i.e. !, #, $, %, &, ', etc.). So you can eliminate using these in an attempt to hack a password.

On all RSTS systems there are accounts that *must* be present. Unless *major* software modifications are made, they *will* exist. Here is a list of these accounts and the default passwords that are used when Digital installs a system.

ACCOUNT	DEFAULT PSWDS(S)	COMMENTS
1,2	DEMO, SYSLIB, SYSMGR, DECMAN	SYSTEM LIBRARY/ SYSTEM MANAGER ACCOUNT
1,3	DEMO	AUXILIARY LIBRARY
1,4	DEMO	
1,5	DEMO	

Of all the accounts, it is most difficult to remove "1,2" due to software requirements, so if you are hacking a system from scratch, it is suggested that you try to work on a password for this account, also note that "1,2" is the system library, and the default system managers account, so the passwords chosen for it sometimes reflect these facts. Also hacking at this account kills two birds with one stone—not only must it be present, but it also has full privileges, as does any account with a project number of 1 (i.e. 1,XXX). Once obtained you will have full access to anything on the system.

Basic System Functions

Once in, RSTS/E will prompt you with 'Ready'. You are now in the RSTS/E 'BASIC' monitor, and you could type in a BASIC program, etc. Here are some useful system commands/programs that can be of use.

HELP—Simply type help. It's available on most systems and fully self-documenting and menu driven. It will give you a complete description of most system commands and functions.

DIRECTORY (or 'DIR')—will give you a listing of programs/files that reside in any account you specify. Simply typing 'DIR' will list the files in the account you are in, to obtain a directory of another account, simply use the format: 'DIR (XXX,XXX)', where 'XXX,XXX' is any valid account number. You can also substitute an '*' in place of either, for a 'match all' or 'Wildcard' search.

SYSTAT(or 'SY')—will give you a listing of who else is currently on the system, what they are doing or running, and some other information. This command is especially useful for obtaining other valid account numbers (PPN's).

OLD—allows you to load a basic program (any file with a '.BAS' extension) into memory. If the program is in the same account as you, simply type 'OLD NAME.EXT', and if the program resides in another account, use the format 'OLD (XXX,XXX) NAME.EXT', where NAME.EXT is the name of the basic program and XXX,XXX is the account/PPN that it resides in.

PIP—is the Peripheral Interchange Program. It is a fancy name for a basic file utility used to transfer files from one place to another. You can get a full description of its uses by typing 'HELP PIP'.

BYE—logs you off the system. Always use this command to log off! If you simply hang up, your account will remain logged on, in a 'DETACHED' state, and this will automatically arouse the suspicion of even the densest sysop, especially if you've managed to obtain a privileged account.

Some Final Notes

Once on under any account, do a directory of all the (0,*) and (1,*) accounts. You will notice a column in the directory listing that is labeled 'PROTECTION'. This is a program/file protection code. It can be set to various levels (i.e. any account can run/list, certain accounts can run/list, etc.). Look for any programs (files with extensions: .BAC, .BAS, and .TSK) which have a protection of (232) or (252). These are programs that give *anyone* who runs them privileges at the time they are run, so make a note of any programs with extensions of this sort and try running/exploring every one. Many programs have *bugs* that can be used to your advantage. This can be discussed in future articles. There is also a program that will allow you to chat with other users on the system. You can usually run it by typing 'RUN $TALK'. It will ask for a 'terminal to talk to', and you can obtain active users/terminals by using the 'SYSTAT' command.

In conclusion, RSTS/E is a fairly user friendly system to use/abuse, and one of my personal favorites. You can learn the basics and become fairly proficient in a relatively short time.

MOBILE PHONES—THEORY AND CONSTRUCTION

by The Researcher

This article explains the operation and construction of a mobile phone. The first section was written in collaboration with another telephone experimenter. It concerned Improved Mobile Telephone Service (IMTS) signaling and was eventually posted on a BBS in the Midwest. From there it fell into the hands of the Chief of Security of Southwestern Bell. His words to the Sysop, who had been busted for Blue Boxing were, "A person with a knowledge of electronics could use the information in that file to build his own mobile telephone." The rest of the article explains how one can be built.

It is presupposed that you have a working knowledge of two-way radio. If you don't possess this knowledge, then you can study up on narrow band FM and 2-Meter transmitters. A good source of information is "The Radio Amateur's Handbook" (readily available from libraries and book stores).

Signaling Used in IMTS

Each mobile telephone channel consists of two frequencies: one for the land base station and one for the mobile phone. The base station uses two tones for signaling: Idle—2000 Hz and Seize—800 Hz. The mobiles use three tones: Guard—2150 Hz, Connect—1633 Hz, and Disconnect—1336 Hz.

The land base station marks the idle channel by placing the Idle tone on it. All the mobiles search for the channel with the 2000 Hz Idle tone and lock on to it.

Each mobile phone is assigned a standard telephone number consisting of area code + 7 digits. When a land customer dials a mobile number, the Idle tone (2000 Hz) changes to Seize (1800 Hz). The number pulsed to the mobile phone contains 7 digits consisting of the area code and last 4 digits of the number. The digits are made up of 50 ms pulses of 2000 Hz separated by 50 ms of 1800 Hz.

If there is a mismatch between the digits sent and the wired ID in the mobile, the mobile drops off and hunts for the idle channel. If the number matches, the mobile will send back an acknowledgement tone of 750 ms of Guard (2150 Hz). The base station waits 3 to 4 seconds for this tone. If not received in that time, the calling party gets a recording. If the tone is received, the mobile phone will ring for up to 45 seconds. Ringing is composed of 1800 Hz and 2000 Hz shifting at 25 ms for two seconds then four seconds of 1800 Hz. When the mobile phone is picked up it sends a connect tone of 1633 Hz for 400 ms to tell the base station it has answered. When the mobile hangs up, it sends Disconnect, which is 750 ms of 1336 Hz. When the base receives the Disconnect tone, it will drop carrier for about 300 ms and go off. If it is the only available channel, it will return to Idle.

What follows is what happens when a call is originated by a mobile: When the mobile goes off hook, it sends 350 ms of Guard (2150 Hz) followed by 50 ms of Connect (1633 Hz). When the base station hears the Connect tone, it removes the Idle tone and stays quiet for about 250 ms. It then transmits 250 ms of Seize (1800 Hz). The mobile then sends 190 ms of Guard and starts transmitting the ID sequence at 20 pulses per second. The ID is the area code and last four digits of the mobile's number. The pulses are marked by 25 ms of connect (1633 Hz) followed by 25 ms of either silence or Guard tone (2150 Hz). If the pulse is odd, it is followed by silence. If even, it is followed by Guard tone. This is used for parity checking. The interdigit time is 190 ms and will be either silence or Guard tone depending on whether the last pulse was odd or even. If the last pulse of the last digit in the ID is even, it will be followed by 190 ms of Guard tone.

When a number is dialed from a mobile phone, 2150 Hz is sent continuously as soon as the dial goes off normal (when the dial is moved from its resting position). Dial pulses representing breaks are marked by 1633 Hz and are sent at 10 pulses per second. A pulse is 60 ms of 1633 Hz with 40 ms of 2150 Hz between pulses.

The most popular mobile telephone channels are located in the VHF high band. Cities are equipped with these channels more than any other band. They are listed below.

Mobile Telephone Frequencies

Channel	Base	Mobile
JL	152.51	157.77
YL	152.54	157.80
JP	152.57	157.83
YP	152.60	157.86
YJ	152.63	157.89
YK	152.66	157.92
JS	152.69	157.95
YS	152.72	157.98
YR	152.75	158.01
JK	152.78	158.04
JR	152.81	158.07

Building the Mobile Phone

This is a list of the components you will need to build your own mobile phone:

1. Cassette Tape Recorder.
2. Radio Scanner (Like those used to receive police calls).
3. Mobile phone dialer (build your own).
4. Low Power Transmitter (Modified 2-Meter transmitter 1-5 watts).

How a Mobile Phone Dialer is Built

Build a Wien-Bridge oscillator to generate the needed tones. These are commonly used in red boxes. If you don't have a red box schematic, look up Wien-Bridge in an electronics textbook. Where you would normally connect a frequency adjustment pot, use two multi-turn pots connected in series. Power for the oscillator will be supplied by a 9 volt battery.

Obtain a rotary dial of the type used on rotary telephones. The dial will have four wires coming out of it: two white, one blue, and one green. The two white wires make a connection when the dial is off normal (moved from its resting position). Connect the two white wires in series with one of the leads from the 9 volt battery. The oscillator will be running only when the dial is moved off normal. It works like this: Dial is moved off normal—circuit is completed between oscillator and battery. Dial goes back to resting position—circuit is opened.

The blue and green wires go to a normally closed contact in the dial. This contact opens once for each pulse in a dialed digit. For example it opens three times for the digit "3". Connect these two wires (blue and green) across one of the pots in the oscillator. With the dial in its resting position, adjust the other pot for a frequency of 2150 Hz (Guard tone). Move the dial until the contact opens and adjust the pot with the blue and green wires going to it for a frequency of 1633 Hz (Connect tone).

When the dial is moved off normal, power will be applied to the oscillator, and it will begin running at 2150 Hz. When the dial is released the short across the second pot will be removed each time the contacts open for a dial pulse. During these pulse times the frequency will shift down to 1633 Hz. When the dial gets back to its resting position, power will be removed from the oscillator. This will exactly duplicate the dial pulsing of a mobile telephone.

The Transmitter

Antennae used by mobile phone base stations are located on high towers. This allows line-of-sight transmission to and from the mobiles. If you are within a few miles of a base station very

(Continued on page 3-28)

British Phonebooth Wedding

Newark Star Ledger

They met in a telephone booth, he proposed to her in it, and the phone company offered them the old-fashioned red box as a wedding present.

In 1982, these two Britons met by chance at the payphone in the northeast England city of Middlebrough. The perspective groom said, "She was taking so long I had to knock on the window to hurry her up." The argument produced a romance, and when he was finally ready to propose marriage, he telephoned her from the same booth.

The couple plan to marry this year and want to put the booth in their garden as a memento.

A British Telecom spokeswoman said, "We would be very happy to give them the kiosk as a wedding present." The old wooden and metal booths, which are being replaced across Britain by modern facilities are normally sold for $200 each.

Man Worries About Sprint Bill

Combined News Sources

Jerry Pepper of Athens, Georgia, panicked when he received a telephone bill for $271,261.91, listing calls to Egypt and Hong Kong, although the phone company assured him that the bill was fraudulent and that he would not be held responsible.

"Traditionally, I'm a worrier," said Pepper. "I was as nervous as can be for a week. I was real bad. Nobody could talk to me. I worried even when they had told me I didn't have to worry."

The bill from GTE Sprint was 646 pages long and showed calls from New York, Baltimore, Dallas, and numerous other locations. One call listed on the bill showed that someone spent two hours and 23 minutes talking to someone in Egypt—which cost $195.

Bad Tenant Databases

The New York Times

Companies hired by landlords to investigate the finances, rent histories, and backgrounds of prospective tenants have begun operating in the New York area.

Tenant groups contend that such investigations, similar to inquiries by credit-rating agencies on people seeking credit, leave renters vulnerable to abuses.

The companies—which identify tenants with such problems as bounced checks, past evictions, or credit shortcomings—say they protect landlords from tenants who have histories of not paying their rents or of causing nuisances that have led to eviction proceedings.

The companies are intensifying their efforts just as the public records of the city's Housing Court are becoming readily available from the court's new computer system. The quick access to the data could also help tenants seeking to determine the record of a potential landlord.

"If you don't get heat or hot water, you have the right to withhold your rent," Mr. Scherer, a lawyer and housing coordinator for Community Action for Legal Services, said. "These computerized systems will tend to make people very uneasy about exercising fundamental rights guaranteed to them by law."

Companies ask their landlord clients to provide the names of tenants who have been evicted. "We're trying to develop a database on people who have actually been evicted, and we hope to have the names of 500,000 such individuals in a year or so," a spokesman for one such company said.

Representative Charles E. Schumer has introduced a bill in Congress to protect tenants against abusive inquiries. No Federal law now shields tenants from the misuse of information. This bill would provide protections similar to the 15-year-old Fair Credit Reporting act, which requires credit-gathering companies to tell consumers why credit applications are rejected and also gives consumers a chance to challenge the accuracy of any data used against them.

One of the nationwide credit reporting companies now marketing advisories to New York area landlords is TRW Inc. Other companies include Data General and Telecheck Services Inc..

Car Breathalizers

Los Angeles Magazine

Thanks to technology and new legislation being introduced in Colorado, it may not be long before those who have had one too many won't be able to *start*, let alone drive, their cars. A bill will be introduced that makes it mandatory for repeat offenders to install a Guardian Interlock System in their car or lose their license. The device, which retails for $295, utilizes the same technology as the police "breathalizer." The problem drinker breathes into a mouthpiece that analyzes the sample with a microprocessor, if the alcohol count exceeds .01, the car won't start.

Phone Phreak Fined

Washington County Times

A 19-year-old New Jersey man has been fined $500 and ordered to pay back $890 in long-distance calls he made at the expense of AT&T.

Robert Davenport of Chippewa Trail was also sentenced to one year probation and directed to get a part-time job within one month.

"My interest is still in telephones and my interest is still in computers, but as far as hacking and phreaking go—not anymore," Davenport said. "Bell is going to be monitoring me like a hawk."

He had been charged with criminal attempt to commit computer-related theft, computer related theft, and theft of services. He pleaded guilty to the latter charge, so the other two would be dropped.

"This is a case where your technical knowledge exceeded your maturity," the judge said. "Until you start acting your age, you're likely to get yourself in trouble again."

Davenport said he did not commit the crime for any financial gain, but only "to continue my existence or my knowledge as a phone phreak."

Marcos Phones For Free

Associated Press

The State Department said it had placed no limit on telephone calls made by former Dictator Ferdinand Marcos while he was a guest of the United States in Hawaii.

A State Department spokesman said he could not confirm reports that Marcos has made thousands of dollars worth of telephone calls from Hickam Air Force Base in Honolulu or that Marcos was trying to influence politics in his homeland by telephone.

[Marcos is now living in a private residence in Hawaii and presumably paying for his phone calls.]

letters...more mail from you...

Dear *2600*:

An issue last fall (September, 1985) described the blue box coding for the verification trunks and gave an example for Michigan (66).

The codes went from 00 to 99. Do you have the ones for area codes 415 and 408?

Telco ANI's for the San Francisco area are 760. If that doesn't work, try "76002222." Right! 8 digits, not 7.

A Reader

Dear Reader:

We hope that someone provides us with a list of area identifiers that correspond to different area codes. But otherwise, there are only ten to choose from: "00", "11", up to "99". So, try them out.

Dear *2600*:

As you can see from the enclosed, I wrote to an associate in Hong Kong (after purchasing all your back issues and subscribing) after reading "1984 arrives in Hong Kong" (Flash, January, 1984). I hope his reply is of help.

Ben Harroll, San Diego, California

Dear Readers:

The article Mr. Harroll referred to mentioned tracking devices that would be installed on all cars in Hong Kong, so that the government could charge for road usage. The following is from the reply mentioned above:

"ERP (Electronic Road Pricing), which is one of the HK (Hong Kong) government's less than inspired ideas said to be costing in the vicinity of HKDLRS 350 million, requires the installation of an entire underground electronic reticulation, with 'viewing stations' positioned at selected points throughout the roads to be 'taxed.'

"These points 'read' specifically designed number plates fitted to the vehicles passing along the roads and the fact recorded for later billing.

"This is totally untested scheme, never been used anywhere else and is being furiously opposed by practically everyone here. There is, in fact, every likelihood that having spent about 35 million in a 'pilot study' the HK government will have to quietly shelve the whole thing.

Dear *2600*:

I noticed one error in your "final words on VMS" (March, 1986). The proper command for changing the default device prior to a directory search is SET DEFAULT devicename: instead of SET DEVICE devicename: as stated in the article. The SET DEVICE command requires OPER privilege and doesn't do what you want anyway. It might also be a good idea to qualify the SHOW DEVICE command (SHOW DEVICE/MOUNTED) so that you don't have to view all terminals, tape drives, etc.

Dear *2600*:

The following is true for Unix systems versions 3.0 and lower.

Unix is set up so that anyone can view anyone else's files unless the user has changed the permissions which rarely happens. This is especially true for the password file. Don't get excited now, this does not mean you can see the passwords, at least not for now. Almost always the password file is under the etc subdirectory which is under the root directory. The command-path is "cat/etc/passwd".

This is excellent for looking for accounts without passwords and finding out user names. The username is followed by a colon then comes the encrypted password. If you see a username with two colons following it that means the account does not need a password. All you have to do to get into these accounts is type the username. No password hacking! Be forewarned that these accounts usually have a very low access level but I'm sure you can work your way around it. C programs are very good to get around this minor obstacle.

A note on encrypted passwords: they are encrypted using a modified version of the DES encryption algorythm. I have heard that it is possible to use the 'crypt' command to decrypt the password if you know the key which I heard is a rather simple default. I have yet to see this work, but we all know anything is possible in this world. Another helpful hint is the 'passed' command which allows you to change a password. Just type the command and the computer will become friendly and guide you through the process.

Heyzeus Arguillis

Dear *2600*:

The day I received my March issue, I started phreaking around with American Express, and I found that the touch tone authorization system is not dead, just a bit different. It's found at 8004324102, 8005225171, and 8005286086. (Numbers to social-engineer are 8003271005 and 8005280682—act like a dumb merchant.) Voice verification is 8005282121. After the initial carrier-like tone, enter 9#, merchant # (10 digits), AX card #, and amount, using pound key ("#") to signal end of input, and instead of a decimal point in the amount of $$ use *. A beep is heard after each input. The lady I spoke to said you can't access an operator on-line.

NYNEX Phreak

Dear NYNEX:

Thanks for the information about how this toy works. We did not say that this service was dead in last month's article (An American Express Phone Story). The author, Chester Holmes, was referring to the ability to get an outgoing dial tone from American Express by using their internal phone system. It is that technique which no longer works.

MOBILE PHONES

(Continued from page 3-26)

little power is needed to establish contact. 1 to 5 watts should be completely adequate. The less power you use, the less your chances of getting caught. More on this later.

2-Meter transmitters, used in amateur radio, operate in the range of 144 to 148 Mhz. With a change of crystals and a little retuning, you have your transmitter.

How A Home Brew Mobile Telephone is Used

With a scanner, locate the base station frequency which currently has the Idle tone on it. Switch to the mobile frequency on that same channel and monitor it with the cassette recorder running continuously. What you want is a clean recording of a mobile unit broadcasting its ID sequence. You also want a recording of the disconnect tone when he hangs up. Once you have these, rewind the tape to the start of the sequence. Now you are ready to make a call.

The Procedure For Placing a Call

1. Set your scanner to the base station frequency with the Idle tone and leave it there. Monitor with earphones to avoid audio feedback through the transmitter.

2. Set the transmitter to the corresponding mobile frequency. Turn it on and leave it on.

(Continued on page 3-29)

A Story of Eavesdropping

Everybody knows an old man who was in the Second World War, and has plenty of war stories to tell. Well sometimes it pays to take the time to listen...

We knew that the enemy was monitoring all of our international radio-telephone channels, despite the sophisticated voice-scramblers which "inverted" speech, making high tones into low ones and vice-versa. Only authorized persons were permitted to use overseas telephone circuits.

We were equipped with elaborate recorders and switching control boxes which permitted us to cut off either side of a conversation, or to substitute ourselves for either party. A strict set of rules forbade us to permit maritime information, weather reports, cargo information, etc. to pass over the circuits.

Influences in Washington sometimes resulted in orders issued to us to permit use of the overseas telephone circuits, even though we were suspicious of previous conversations because parables and unusual phrases often used, made it difficult to follow what was being said. "How can we monitor carefully, when we can't understand what they're saying?" went unheeded.

We caught one fellow red-handed in South America using weird terms like "birds leaving the nest with a basket of eggs". I finally cut in the circuit and told him I'd forgotten what they meant. He tried a couple of other phrases which I also couldn't understand. Finally, he lost his patience and blurted out, "Oh hell, I'm talking about those special munition orders which left yesterday for Germany."

By this time, a special telephone speech scrambler had been developed which was small enough to fit and use on a desk. Its availability was extremely limited, but a couple of Army officers—one in the U.S. and the other in Panama—had been able to get hold of a pair of them, and between them secretly installed them on their desks, unbeknownst to us of course!

One day I heard the fellow in Panama say "OK Joe, now over to the scrambler" and their ensuing conversation became unintelligible. We quickly checked the radio telephone circuit equipment and discovered that the technical characteristics of the equipment they were using and our own was identical. As a result, when they inserted their scramblers the speech inversion righted itself and their conversations went out over the radio-telephone circuit in clear language—readable by anyone!! That was the end of the use of their private "secret conversation system".

Some of the worst offenders of overseas telephone use security were the top people. I'll have to list Generals Eisenhower and Marshall as two of them—at least sometimes. I can remember one day the circuit between London and Washington happened to be very poor in quality and "understandability" was stretched to the utmost.

General Marshall in Washington had General Eisenhower on the line in London who couldn't understand a word of what Marshall was saying. Marshall repeated several times "Ike, this is GCM—Marshall—GCM—got it?" without results. Finally in frustration Marshall turned to an aide and could be plainly heard to say "What's the code word for my name?"

The next thing we knew, Marshall was slowly and distinctly repeating his code name interspersed with "GCM" and "Marshall". Of course, we had to cut the circuit and notify the code group in Washington to immediately "bust" the code—we couldn't take any chances—revelation of the code word for his name might have been all the enemy intelligence was waiting for to help it "code-break" other communications.

On the other hand, President Roosevelt and Prime Minister Churchill were two of the best and easiest to monitor. Both used references to previously transmitted overheard messages by numbers and most of the conversations were along the lines: "Well Winnie, on number 528, I really don't think we should do that—you know how they are." Nobody could gain any information from listening to their telephone conversations.

I always enjoyed listening to Sir Winston originating a call. The British telephone operators were required on *every* connection to announce in advance of a conversation: "You are warned not to mention the names of vessels, sailing dates or conditions, cargoes, weather, etc., etc., etc.—any violation on your part will result in the circuit being cut off and your action being reported to the highest authority. Do you understand?" Sir Winston always docily replied, "Yes ma'am, I understand."

One enemy group had learned the "language" of speech inversion. For example, listening on the air to a radiotelephone circuit, one might hear a word that sounded exactly like "*krinkanope*"; that was the word "*telephone*" after it had passed through the speech inversion system!!!

2600 (ISSN 0749-3851)

Editor and Publisher
Twenty Six Hundred

Associate Editors
Eric Corley
David Ruderman

Executive Director
Helen Victory

BBS Operator
Tom Blich

Writers: Paul Estev, Mr. French, Emmanuel Goldstein, Chester Holmes, The Kid & Company, Lex Luthor, Lord Phreaker, Mike Salerno, The Shadow, Silent Switchman, and the usual anonymous bunch.

2600 is published by 2600 Enterprises, Inc., an electronoetary organization.
ANNUAL SUBSCRIPTION RATES: $12, individual; $30, corporate; $20, overseas.
LIFETIME SUBSCRIPTION: $200 CORPORATE SPONSORSHIP: $2000.
BACK ISSUES: $2 each, individual; $3 each, corporate; $2.50 each, overseas.
MAKE CHECKS PAYABLE TO: 2600 Enterprises, Inc.
WRITE TO: 2600, P.O. Box 752, Middle Island, NY 11953-0752.
TELEPHONE: (516) 751-2600. BBS: (201) 366-4431.
ADVERTISING DEPARTMENT: P.O. Box 762, Middle Island, NY 11953-0762.
ARTICLE SUBMISSION AND LETTERS: P.O. Box 99, Middle Island, NY 11953-0099.
POSTMASTER: This is a privacy mail.

MOBILE PHONES

(Continued from page 3-28)

3. Play the taped ID sequence.

4. Use your dial pulser to call the desired number. If all has gone well, you will hear your dial pulses in the earphones. You can use this method to call one of the special 800 numbers and whistle off with 2600 Hz; then MF to anywhere in the world. This technique will reduce your visibility on the bill for the ID you are using.

5. When you are ready to hang up, play the disconnect tone and switch off the transmitter.

A Few Notes About Your Own Security

You should use only as much transmitter power as necessary to maintain a reliable contact. If you do much of this kind of experimenting, the FCC is going to be after you with direction finding equipment. These use directional antennae and a process of triangulation to locate illegal transmitters. If you keep your power down, stay mobile, and avoid establishing a pattern of calling at the same time every day, it will be nearly impossible to track you down.

This file was kindly presented by P-80 Systems for entertainment and academic study only. It is a violation of Federal laws to operate an unlicensed transmitter.

This month at 2600

More on **Private Sector BBS**: We have obtained some very interesting information that we hope will allow us to conclude our study of this fascinating case. The information takes the form of two transcripts of proceedings to obtain search warrants. The first transcript concerns a search warrant for a computer that was seized in New Jersey just before the Private Sector was seized on July 12, 1985. It was "evidence" from this first warrant that permitted the second, more well known, raid of seven computers. The second transcript is the proceedings that permitted the seizure of The Private Sector and the others.

We don't have the room to print these documents here, but we can print a few excerpts. Both transcripts have been kindly keyed by some mad typists into computer readable form. They are now available on the 2600 office BBS (5167512600, Friday and Saturday nights only from 12 midnight until 12 noon only) and, of course, on The Private Sector (2013664431). Hardcopy printouts or an MS-DOS disk containing these transcripts are available from *2600* for $5. We hope you read these transcripts and spread them around the country. They mention the usual: credit card fraud, toll fraud, theft of service, computer fraud, and countless permutations. In them there is no mention of the control of satellites, the ordering of tank parts, or the spread of secret Pentagon phone numbers. It took Middlesex County Prosecutor Alan Rockoff the whole weekend after the computers were taken to come up with these fairy tales. Taking the form of typical judicial-type questions and answers, the documents give insight into how law enforcement officials think (or don't think). They reflect the classic example of an unexperienced government (unexperienced with dealing with computer related issues) stumbling over people's rights. Here are some of the good parts:

Why did they pick on these seven people?

A. We narrowed the list down to the seven [out of 130 possible "suspects"] who we feel are the main offenders along with Mr. XXXXXXX and his bulletin board service by utilizing his records, reading his messages from these people that they have posted on his bulletin board and also by calling these bulletin boards up utilizing Patrolman Grennier's computer and obtaining information from their computer.

And now here is the "evidence" which allowed them to break into the homes of seven New Jersey computer hobbyists:

Q. And this number [referring to another victim of this farce] also is a—is it a bulletin board?

A. All right. We did not get through to this number, however, by the way it's busy it appears to be a bulletin board. Once we did get through we got a carrier but my computer was not set up to receive it so there is a computer on line there and by the way it's busy it's characteristic of a bulletin board system.

How's that for conclusive evidence?

Q. What information did you receive from Mr. XXXXXXX's programs that would indicate that the computer at 757-XXXX was being used for illicit purposes?

A. He was giving information on how you could tell—if you were into the phone company they were tracing you so that if you were calling illegally you would know for a fact that you are being traced. He also gave directions on a diverter and how it works with complete information.

Q. What information did you obtain from this particular number [yet another number]?

A. He gave something known as 800 codes along with an—he also gave a number for conference calling. I believe that's what that was.

Q. What information did you receive from 469-XXXX?

A. All right. Through him we received a conference call number. He also gave you information on how AT&T traces numbers. He tells you, like, for example, there was one number given out on the bulletin board for conference calls which is 950-1088 and he explains to you how that is traceable. You should not use that number because a lot of people are getting caught. He also states that if you call him he will give you a list of Sprint access numbers and he gives a phone number to call.

Sprint access numbers are passed around quite gladly by Sprint. Conference call numbers are also public knowledge. Information on tracing is not illegal either.

Q. What information did you get off of Mr. XXXXXXX's bulletin board that would indicate that Red Barchetta is using this computer for illegal purposes?

A. He explains to you how to make mace, a CO2 canister bomb, unstable explosives, a jug bomb, a smoke bomb, something known as a rocket engine bomb and he goes into how to use household items to make those and the correct mixtures for making same.

Even these people couldn't deny that the 1st Amendment allows for this kind of thing. So here's how they got around that little hindrance:

THE COURT: Well, what's wrong with telling the whole world on how to make bombs in their kitchen?

PATROLMAN GRENNIER: Well, number one, is the possibility that someone who was not readily accessible to that information now has it much freer and that type of person may be more likely to use it. In other words, it's right there now. It's not something that they have to research.

And for those BBS operators out there who somehow think disclaimers serve any advantage at all...

Q. Okay. What other questions did they ask you for the access?

A. If I was a law enforcement officer, if this was part of an entrapment, and the third question if this was a trap.

Q. And you had to respond to those questions?

A. That is correct.

Q. You responded in the negative?

A. That is correct.

***

Since The Private Sector was returned, it arrived with something interesting. There was a new, updated userlog, which listed the logons that were attempted while the computer was in the hands of Middlesex County. The order of the logons subsequent to the seizure of the equipment were: QQQQQQQQ, 2600 MAGAZINE, MIDDLESEX COUNTY PRO, 2600 MAGAZINE (3 times), KID & CO., 2600 MAGAZINE (2 times), BROADWAY HACKER, LEX LUTHOR, LOGIC GOD, PRIVATE SECTOR, JOHN DOE (4 times), GRIM REAPER, JOHN DOE (3 times), HEADRUSH, FOREST RANGER, FLYING DRAGON, JOHN DOE, COL. HOGAN, JOHN DOE (3 times), PRIVATE SECTOR, EVIL RABBIT, SHADOW 2600, DOCTOR DEMENTO, DOCTOR WHO, DOCTORK, JOSHUA, ERIK BLOODAXE, KERRANG KHAN, KID & CO., DAVID LIGHTMAN, JOHN DOE (6 more times). You can derive what you want from this. The userlog shows that the first few users in this list "used" the system for half-hour periods, up to almost two hours for one of the JOHN DOE logons. After GRIM REAPER they used the system between 1 and 15 minutes for each logon. The logons are date-stamped from 7/12/85 to 8/13/85, but we are told that the internal clock may have screwed up the dates when the computer was taken....Other office notes: we are still investigating that "magazine" called ***Computel***. We already have much information on them but in another month we should have

(Continued on page 3-32)

SYSTEMATICALLY SPEAKING

617 Will Be Divided

UPI News Service

In 1989, area code 617 (Boston) will be split to provide more phone numbers. The western part of the area code will remain the same while the rest will have a new, as yet undetermined area code.

Congress Chooses AT&T

New Jersey Herald News

Chesapeake & Potomac Telephone Co., the local Washington area Bell affiliate that has had the congressional phone contract for the past 107 years, is bitterly contesting a House Administration Committee decision to reach out and touch AT&T for its future phone needs.

Representative Charles Rose said that AT&T's offer was simply better particularly because all the phone-switching equipment would be located on Capitol Hill grounds. C&P would have its switches in another part of the city.

"All conversations will remain on Capitol Hill," said Rose, citing security threats of electronic eavesdropping.

Baby Bells Don't Pay AT&T Bills

MIS Week

AT&T has filed for the recovery from its former Bell offspring of more than $87 million for failure to properly bill and collect revenues due it from end-users following the switch to an access-charge billing system after divestiture.

AT&T said the lion's share of the burden, about $40 million, is due from New York Tel. An AT&T spokesman said the amounts are now being formally claimed because of a two-year statute of limitations on such claims.

Other claims range from $7 million against New England Telephone down to $330,000 from Nevada Bell.

Since divestiture, the local Bell Operating Companies have handled billing for most long distance and some private-line services. AT&T said the claims are a legal procedure, adding that "whenever another company handles billings of that magnitude, you're bound to run into problems."

In the complaint, AT&T said that in the case of New England Telephone, it had been "deprived of revenues" by "various acts and omissions," including the failure of New England Telephone to "properly record, assemble, edit, or process details of switched services calls placed by AT&T Communications' end users."

Other charges were that the telco failed in some instances to properly prepare and process bills for message-billed and bulk-billed services, and some private-line services.

Equal Access 800 Drawbacks

Communications Week

Over the next six months, the Bell operating companies and some independent telephone companies will spend millions of dollars to make an 800-type service available to AT&T's long-distance rivals.

But despite the costs, the type of 800 service they'll be able to provide will represent an interim offering that will be inferior to AT&T's.

In fact, some of AT&T's rivals are unsure they will be able to use the service, are uncertain they will benefit from it, and are unconvinced their customers will buy it.

Under terms of the divestiture, the BOC's are required to provide all long distance companies with access equal to AT&T's and that includes access to 800 service, one of the nation's fastest growing long distance products. But the BOC's won't have the technical capability to offer service equal to AT&T until 1988.

800 numbers were functioning so well before the divestiture because AT&T used common channeling interoffice signaling (CCIS), which looks at the 800 number dialed and translates it into an entirely different number—the number of the called party. Now the BOC's have to develop their own method of replicating CCIS.

Encryption Provides Signature

Infoworld

A data encryption scheme promises to offer increased security as well as a way of authenticating messages sent over a local area network, according to the manufacturer.

Mailsafe is the first microcomputer security system to rely on individual public and private "keys," said Barton O'Brien, vice president of sales for RSA Data Security. The system will permit users to make one of their keys available to anyone, while keeping the other confidential. The publicly available key can then be freely used to encrypt a file that can be decoded only by using the matching private key. In Mailsafe, public keys are maintained in a database that is incorporated in the program.

"This is really the same thing as providing a digital envelope," O'Brien said. The system also provides the equivalent of an electronic signature, he said. A sender can use his private key to encode a message that can be successfully decoded only by the matching public key, so the recipient can determine the authenticity of a message. The "signature" will allow computer users to transmit information, such as that in a legal or financial document, that was previously limited to paper transactions to verify the authenticity, he said.

Mailsafe is based on the patented RSA Public Key Cryptosystem. The algorithm was developed at the Massachusetts Institute of Technology in 1978.

Directory Assistance Failure

Newark Star-Ledger

Earlier this year, operators in four directory assistance offices in area code 609 could not get into their data bank to find telephone listings because of a computer failure.

As a result, the operators were forced to look up inquiries manually in phone books—and only for emergency requests.

An estimated 50,000 directory assistance calls were affected.

Dial "00" For Operator

MIS Week

Very soon, customers of Pacific Bell will have to dial "00" to reach the standard AT&T operators. If they dial "0" they will reach new Pacific Bell operators.

The change is part of the divestiture. It was decided that the Bell Operating Companies would provide their own operators, primarily for assisting callers in making intra-LATA calls.

This part of the breakup will require AT&T to give up its precious "0".

THIS MONTH

(Continued from page 3-30)

enough to start getting some refunds as well as find out who, if anyone, is commanding them. For now, we can tell you that these people are definitely the same ones behind the magazine which came out in the mid seventies called *Tel*. That magazine was busted by the phone company for publishing "trade secrets". Now the same people are back, only this time it's phones *and* computers in a magazine that never comes out and has access to a whole lot of money. A curious situation indeed. Much thanks to the 2600 West Coast investigative team for what they're about to do....Yes, we were supposed to announce our meeting time and place in this month's issue. But we've had a surprising lack of input from our readers. We want to have a meeting in New York and other cities. But we need to know if people are interested enough to attend. We also need help getting a room for such an event—nothing special; a meeting room at any college would do just fine. Call us—we'd like for you to be a part of the many changes we have planned....Regarding the problems we mentioned last month about Compuserve, we recently received a full refund. Let's all hope they learned their lesson. □